

My



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/516,910	03/01/2000	Dan Boneh	APP1245-US	3127

9941 7590 03/26/2004

TELCORDIA TECHNOLOGIES, INC.
ONE TELCORDIA DRIVE 5G116
PISCATAWAY, NJ 08854-4157

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 03/26/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application

09/516,910

Applicant(s)

BONEH ET AL.

Examiner

Beemnet W Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 March 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 40-53 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 40-53 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 40-53 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 40-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Joye et al. [Ref U] (hereinafter referred to as Joye) (UCL Crypto Group Technical Report Series, Further results on Chinese Remaindering, March 7, 1997).

4. As per claim 40, Joye teaches a method of determining a secret information in a cryptography device, the method comprising:

generating an electrical signal comprising a stream of bits (messages M1, M2) containing a correct digital signature in a cryptography device (page 2, paragraph 3, lines 1-2);

placing the cryptography device under physical stress (damaging the device) and in response to the physical stress, generating an electrical signal comprising a stream of

bits containing an incorrect digital signature in the cryptography device (page 2, paragraph 3, lines 3-4);

determining secret information q stored in said cryptography device using:

$\gcd(E-E', N) = q$, [page 2, paragraph 3, line 5, and page 3, preposition 1]

generating an output electrical signal comprising a stream of bits containing the secret information used to generate the correct signature (page 3, preposition 1, last line).

Joye does not explicitly teach utilizing two different devices to generate the secret information. It would have been obvious to one having ordinary skill in the art at the time the invention was made to implement a method of using two devices to generate a secret information into the secret generation method of Joye so that the secret can be generated using two devices.

5. As per claim 41, Joye teaches a method of determining secret information in a cryptography device as applied to claim 40 above. Furthermore, Joye teaches the method, wherein the device generates a digital signature which may be separated in to linear components (i.e. signatures s_1 , and s_2) [page 2, paragraph 3, lines 1-2].

6. As per claim 42, Joye teaches a method of determining secret information in a cryptography device as applied to claim 40 above. Furthermore, Joye teaches the method, wherein placing the said first cryptography device under physical stress

includes at least one of applying atypical voltage levels, applying a higher speed, or applying radiation (i.e. damaging the device) [page 2, paragraph 3, line 3].

7. As per claim 43 Joye teaches a method of determining a secret information in a cryptography device, the method comprising:

in a cryptography device, generating an electrical signal comprising a stream of bits containing a first authentication value of form $r^2 \bmod N$ wherein r is a random number and N is a secret value which is a product of prime numbers (page 2, paragraph 2, lines 1-2, and paragraph 3, lines 1-2);

in a cryptography device, generating an electrical signal comprising a stream of bits containing a subset of integers S (page 2, paragraph 3, lines 1-2);

in a cryptography device, generating an electrical signal comprising a second erroneous authentication value device (page 2, paragraph 3, lines 3-4);

determining secret information based on calculated values (page 2, General model, and page 3, preposition 1).

Joye does not explicitly teach utilizing two different devices to generate the secret information. It would have been obvious to one having ordinary skill in the art at the time the invention was made to implement a method of using two devices to generate a secret information into the secret generation method of Joye so that the secret can be generated using two devices.

8. As per claims 44-48, Joye teaches a method of determining secret information in a cryptography device as applied to claim 43 above. Furthermore, Joye teaches the method wherein generating the secret value involves calculated values based on two prime numbers p and q and module n being the product of the two prime numbers (page 2, General model, and page 3, preposition 1); and generating a plurality of signatures comprising a subset of integers S (page 2, paragraph 3, lines 1-2);

9. As per claims 49-53, the claimed steps correspond to the functions of the elements of the method claims 44-49, which has been rejected above and thus rejected with the same reason applied thereto.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a) U.S. Patent No. 5,991,415 to Shamir teaches a method and apparatus for protecting public key schemes from timing and fault attacks.
- b) Eli Biham et al. Internet article teaches, How to break completely unknown cryptosystems.
- c) Floyd et al. teaches Differential fault analysis.
- d) Joye et al. teaches a method of attacks on systems using chinese remaindering.

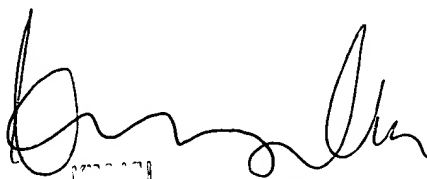
11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

March 19, 2004



10/13/03
SUPERVISOR OF THE EXAMINER
10/13/03